INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2024, VOL. 70, NO. 4, PP. 1005-1011
Manuscript received June 20, 2024; revised October, 2024. doi: 10.24425/ijet.2024.152088

Evaluating the steganographic integrity of the phase coding method for concealing confidential information within audio files

Ruslana Ziubina, Valentyna Teliushchenko, Olga Veselska and Andrii Petrenko

Abstract— **Despite advancements in encryption technology, the issue of covert data transmission remains relevant. Researchers are actively enhancing established methods of concealing information with software tools that utilize mathematical models and developing new data entry methods. Steganographic techniques can be used with cryptographic methods to enhance the confidentiality of information within a container or as a standalone software tool. This article examines the steganographic integrity of concealing confidential information within audio files. The steganographic technique was selected as the phase coding method, which involves substituting the audio element's phase with the secret message's relative phase. An implementation of the chosen method was developed for the experiment. During the experiment, secret data of varying lengths were used to assess the impact of the length of the concealed information on the distortion of the audio file that may be perceptible to the listener. The study also investigated the resilience of the concealed information to noise attacks, allowing for the determination of the threshold of its robustness. The findings provide insight into the reliability of this steganographic method for hiding classified information within media objects.**

Keywords—**phase coding method; steganography; confidential information; attack; audio file**

I. Introduction

PROTECTING digital information against unauthorized access has become a crucial concern due to the rapid advancement of technologies for processing and reproducing various signals, including text and multimedia data. Cryptography is a widely used approach for information protection. It involves transforming the information using key data to obscure and restore the content of information and ensure its authenticity, integrity, and authorship, among others. Cryptography converts information into an incomprehensible form, thereby concealing the content of messages through encryption. Consequently, the relevance of cryptographic methods has grown due to the need to secure digital information resources.

Steganography is a method of hiding information, which aims to conceal the existence of secret information during its transmission, storage, or processing. The key objective of a steganographic system (SS) is to embed a message within a container in such a way that third-party observers can't distinguish between the original and modified objects. Key features of an SS include security, stability, indistinguishability, and throughput (for a steganographic channel). One critical characteristic of steganography is "imperceptibility," which refers to the requirement that data must be inserted into the container without being detectable by human senses. This can be achieved by making minor modifications to the stegano-container or by utilizing properties of human senses, such as utilizing frequencies or modifications below the absolute threshold of human hearing for audio steganography.

This article presents a steganographic technique for data hiding in audio files. The experiment is conducted using the WAV digital format as the multimedia container, although the results and recommendations are applicable to other audio formats as well. The study investigates the robustness of the hidden message against an attacker who attempts to silence the audio file. The steganographic phase coding method is used in this work, which involves replacing the original audio element with a relative phase representing the secret message. This method relies on the human ear's receptive characteristics, specifically the small changes in the phase of the signal that are imperceptible to the human auditory system. The total phase of an oscillatory argument describes an oscillatory process as a periodic function [19].

Compared to other methods investigated, the probability of distortion of secret information in this method is much lower. Thus, a proprietary software product is developed to ensure the protection of embedded information in audio objects using this method. The growing interest in multimedia technologies and the need for steganography further highlights the significance of this study. With Python software and audio media in the form of a media file, the study continues previous research on steganography, including the phase coding method.

The experiment evaluates the distortion of the audio container after introducing a hidden message to assess the multimedia data quality using temporal and spectral characteristics. The study determines the stability threshold of hidden information at different signal-to-noise ratios (PSNR). Therefore, this article aims to investigate the steganographic stability of hiding confidential information in audio files using the selected phase coding method.

The first Author and third Author are with the University of Bielsko-Biala, Bielsko-Biala, Poland (e-mail: rziubina@ubb.edu.pl, oveselska@ubb.edu.pl).

The second Author and fourth Author are with National Aviation University, Kyiv, Ukraine (e-mail: telyushchenko@bigmir.net, pab.05@ukr.net).

II. Literature review

Audio steganography is the art of hiding secret information within an audio signal in a way that is imperceptible to the human senses. Among the various steganography techniques, the phase coding method has been widely adopted due to its high embedding capacity and low distortion. In this literature review, we examine several recent papers that propose modifications and hybrid techniques based on the phase coding method to achieve higher embedding efficiency, security, and robustness.

The first paper [1] proposes a novel approach to steganography that uses the phase coding method with improved embedding efficiency compared to traditional methods. The authors demonstrate that their method achieves higher embedding efficiency, meaning more data can be hidden within an audio signal while maintaining low distortion. This is an important contribution to the field of audio steganography as it offers a more efficient way to embed hidden data within an audio signal.

The second paper [3] provides an overview of the phase coding method and proposes a modified approach to increase its embedding capacity. The authors point out that the phase coding method has several advantages over other steganography techniques such as high embedding capacity and low distortion. However, the method has some limitations in terms of embedding capacity. The authors propose a modified approach to overcome these limitations and increase the embedding capacity of the technique.

In [4], Zhongling Liu et al. propose a new steganographic method that combines phase coding with key modulation for high capacity and security. The authors highlight the advantages of their proposed method, including higher capacity, robustness against noise, and security against attacks.

Juan Núñez et al. propose a novel approach in their paper [5] that combines phase coding with echo hiding to improve the robustness and security of the steganographic method. The authors show that the proposed method achieves higher security and robustness compared to other steganography techniques.

Yonghong Yuan et al. propose an audio steganography method in their paper [6] that uses phase coding and spectrogram analysis to achieve high capacity and low distortion. The authors demonstrate that their proposed method achieves higher capacity while maintaining low distortion.

In [7], Yuling Yang and Shijie Jia propose a hybrid technique that combines phase coding with a modulation method for high capacity and security. The authors highlight the advantages of their proposed method, including high capacity, robustness against noise, and security against attacks.

Finally, Ruoyu Li and Xiaolong Li propose two papers titled "An Audio Steganography Scheme Based on Phase Coding with High Embedding Capacity" and "Steganographic Method for Audio Signals Based on Phase Coding with High Embedding Capacity". Both papers [8-9] use the phase coding method to achieve high embedding capacity while minimizing distortion. The authors highlight the advantages of their proposed method, including higher capacity, low distortion, and robustness against attacks.

Overall, these sources demonstrate the versatility and effectiveness of the phase coding method for audio steganography. The proposed modifications and hybrid techniques provide new possibilities for the use of steganography in various applications, including secure communication and digital rights management. These papers highlight the ongoing development in this field and provide valuable insights for researchers and practitioners interested in audio steganography.

III. Methods

The technique of phase coding involves modifying the phase of an audio signal to conceal embedded information. This is achieved by replacing the phase of the primary sound segment with a reference phase that represents the hidden data. When possible, phase coding is considered one of the most efficient coding methods in terms of the signal-to-perceived noise ratio.

A significant change in the phase ratio between each frequency component results in a substantial phase dispersion. However, if the phase modification is small enough, stealth can be achieved, which is imperceptible to human hearing. It should be noted that the threshold for perceptibility varies among observers, with spectral analysis specialists able to detect changes that appear insignificant to the average listener.

To implement phase coding, the audio signal is first divided into segments $(S\_0, S\_1, \ldots S\_(n-1))$. The phase of the initial segment conveys the encoded message, while the phase of the subsequent segments is adjusted to ensure that the phases are indistinguishable from each other, or at least difficult to differentiate.

Let's consider the process of extracting the encoded message. To obtain the secret message from the file, it is necessary to use a special detection function:

$$q = \Sigma\, r_i\,(v_i - \varphi_i)^2 - r_i\,(u_i - \varphi_i)^2 \tag{1}$$

Where:

- $u = \{\alpha_0, \beta_1, \alpha_2, \beta_3\}$ – the received signal;
- r_i – the amplitude of the i-th generated signa;
- φ_i – the phase of the i-th generated signal;
- $u = \{\alpha_0, \beta_1, \alpha_2, \beta_3\}$ – expected/predicted sequence of phases in the case of single coding;
- $v = \{\alpha_0, \beta_1, \alpha_2, \beta_3\}$ – expected/predicted sequence of phases in the case of zero coding;
- α_i, β_i – phase values (closest) corresponding to zero and one.

Using the presented formula, we can find the value of q. Depending on its value, we can determine whether a zero or one is encoded in the transmitted message. If it is greater than zero, the bit of the transmitted message equals one, and if it is less than zero, the bit equals zero accordingly [14-18].

While the phase coding method has advantages, such as being imperceptible to human hearing, several disadvantages should be considered. These include:

1. Vulnerability to noise: Phase coding is highly sensitive to noise in the audio signal, which can disrupt the phase relationship between frequency components and cause errors in the decoding process.

2. Limited capacity: Phase coding has a limited capacity for embedding data compared to other steganographic methods, such as frequency domain techniques. The amount of data that can be hidden in the phase of an audio signal is proportional to

the number of frequency components, which is often limited by the sampling rate of the audio signal.

3. Complexity of implementation: The implementation of phase coding requires significant computational resources and expertise in signal processing and steganography. This makes it less accessible for non-experts and can increase the risk of errors in the embedding and decoding process.

4. Susceptibility to detection: While phase coding may be imperceptible to human hearing, it can be detected using advanced signal analysis techniques. A skilled analyst may be able to identify changes in the phase relationship between frequency components, which can indicate the presence of hidden data.

Overall, the limitations of phase coding make it a less desirable choice for steganography in some applications. Careful consideration of the specific requirements and constraints of the application is necessary to determine whether phase coding is an appropriate technique.

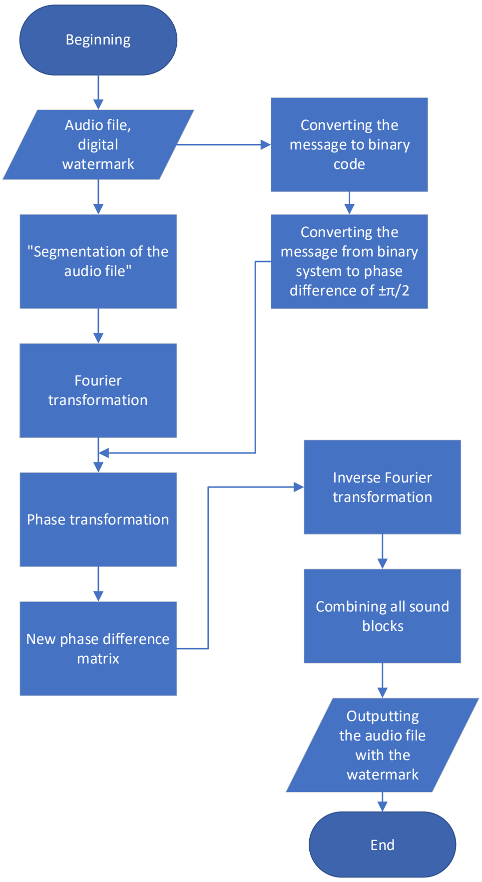


Fig. 1. Block diagrams of the encoder

A steganographic method was employed to conceal information within selected audio files, and software was developed in Python programming language to implement the technique. Python was chosen due to its cross-platform compatibility, simplicity, and access to a large number of libraries. Block diagrams of the encoder and decoder were constructed to guide script program development, and are depicted in Figure 1-2.

For the experimental setup, a 15-second audio file was selected as the steganocontainer, with a sampling frequency of 44100 Hz, two channels (i.e., stereo signals), a file type of WAV, and a size of 2.56 MB. The message "telyushchenko" was used as the secret information, which was repeated to facilitate the comparison of results.

After completion of the program, the output signal was confirmed to be a complete steganocontainer with the same file type (WAV), indistinguishable from the original by human perception. The original signal, along with its temporal and spectral representations, and the modified signal containing the hidden message (also with its temporal and spectral representations) were constructed using the MATLAB application program package [19-22].

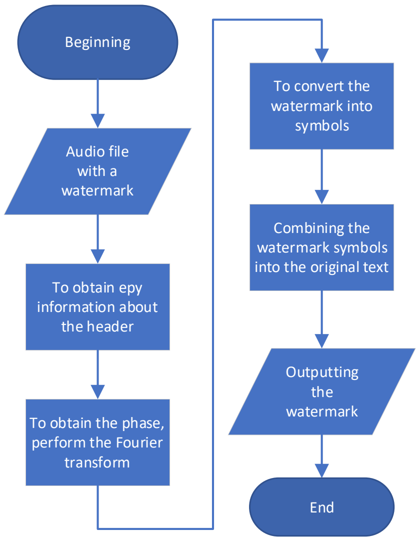


Fig. 2. Block diagrams of the decoder

After completion of the program, the output signal was confirmed to be a complete steganocontainer with the same file type (WAV), indistinguishable from the original by human perception. The original signal, along with its temporal and spectral representations, and the modified signal containing the hidden message (also with its temporal and spectral representations) were constructed using the MATLAB application program package [19-22].

A. Embedded information resilience to noise attack

One of the most common attacks is the signal noise attack. In audio engineering, the signal-to-noise ratio is determined by measuring the voltage of noise and signal at the output of an amplifier or other sound reproduction device using a root mean square millivoltmeter or spectrum analyzer. Noise determines the probability of error in message transmission over a communication channel and, ultimately, the channel's bandwidth. In digital signal processing, additive white Gaussian noise is most commonly used. Additive because it is summed with the useful signal [22-26].

White noise is a stationary, random process with uniformly distributed power density. It has components that change rapidly, slowly, and moderately, and none dominates the others. Named by analogy with white light due to the presence of all spectral components. White color is obtained by adding all other colors of the visible spectrum. If the analogy continues to use the visible range of waves, a certain color can denote the predominance in the spectrum of certain signal components.

One of the quality system properties is the signal-to-noise ratio. This dimensionless quantity equals the ratio of useful signal power to noise power. This ratio is often measured in decibels (dB). The higher the value, the better. One of the tasks of digital signal processing is to increase the signal-to-noise ratio.

During the study, Gaussian noise with different signal-to-noise ratio values was added to our audio file with embedded messages to determine the threshold of embedded information resilience to noise attack.

IV. Results

A. Evaluation of the information-hiding program result using the phase coding method

Figures 3-5 illustrate the results of the program's operation for embedding and extracting hidden messages of various lengths using the phase coding method into our audio file. Messages of lengths 13 and 1000 characters were chosen to track container distortion perceptible to the human ear and to assess the increase in file size when embedding information.

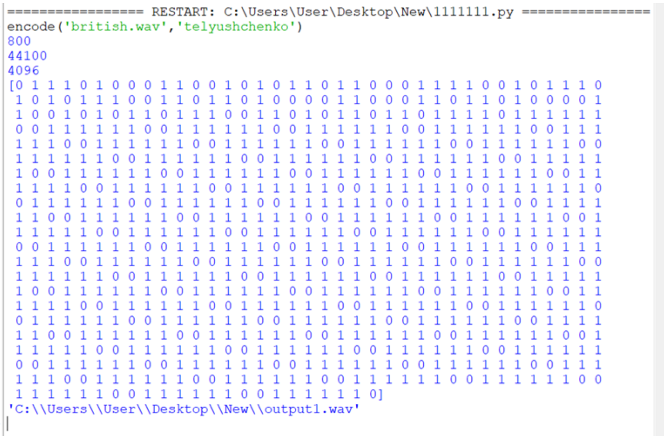


Fig. 3. The result of executing the encoding script for embedding the message "telyushchenko," consisting of 13 characters

Fig. 4. The result of extracting the message from the steganographic container

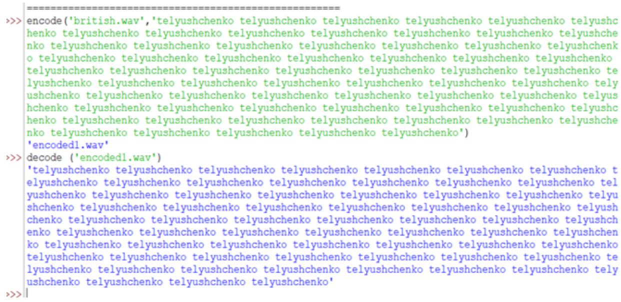


Fig. 5. The result of the program for embedding and extracting a message with a size of 1000 characters from the steganographic container

As evident from the presented results, the program successfully embeds and extracts the hidden message without distorting it during extraction.

B. Comparison of diagrams of empty and filled steganographic containers with different message lengths

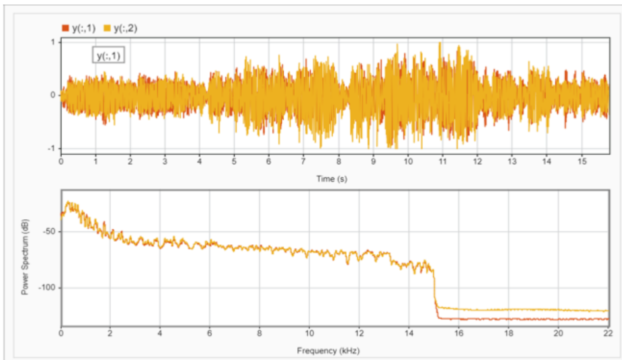


Fig. 6. Temporal and spectral representation of an empty steganographic container

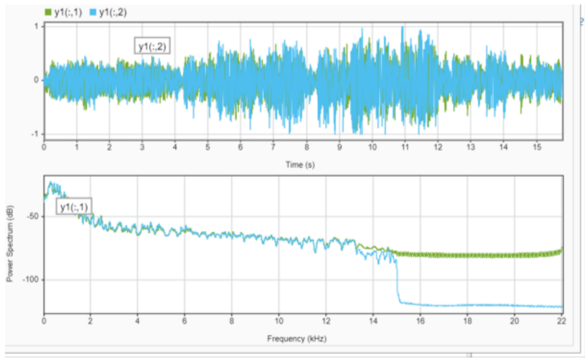


Fig. 7. Temporal and spectral diagrams of a filled container with a message size of 13 characters

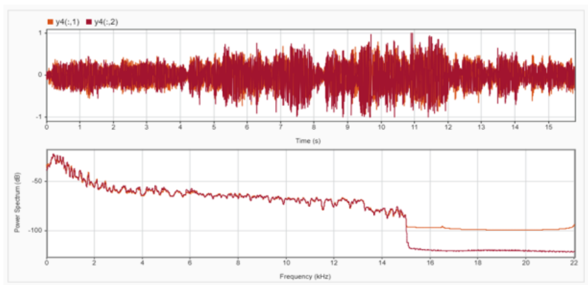


Fig. 8. Temporal and spectral diagrams of a filled container with a message size of 1000 characters

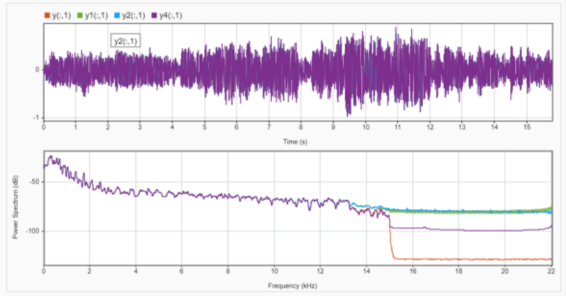


Fig. 9. Comparison of diagrams of empty and filled steganographic containers with different message lengths

The obtained results allow for the following observations. As seen from the diagrams above (Fig. 6-9), it can be emphasized that the difference between an empty audio container and a container with an embedded message conforms to the standards of this method and differs only in the spectral domain of the upper frequencies of the first channel. Thus, our message was embedded in the upper-frequency region of the first channel. However, distinguishing between an empty audio file and a file with embedded messages by ear alone is impossible without decomposing the filled steganographic container into its spectrum.

Furthermore, the change in the size of the audio file with embedded messages of different lengths was analyzed. This information is presented in Table 1.

As seen from Table 1, with a small message size, the size of the steganographic container remained almost unchanged. However, as the message size increased, the size of the steganographic container also increased. This leads to the conclusion that a steganalyst may suspect the presence of embedded information in the steganographic container only by comparing the file size of the original and obtained files.

TABLE I
THE SIZES OF THE AUDIO FILE WITH DIFFERENT AMOUNTS OF EMBEDDED DATA

Message Size	Audio File Size (MB)
Empty Container	2,65
13 characters	2,67
100 characters	2,67
1000 characters	3,00

Regarding the extent of audio file distortion when embedding messages of different lengths, no distortions in our steganographic container perceptible to the human ear were detected in our three cases. Perhaps distortions may become noticeable when embedding information of a large volume.

C. *Experimental evaluation of the hidden message's resilience to noise attack*

To determine the resilience threshold, the MATLAB software package was utilized to add white Gaussian noise to our audio file with the embedded message. The noise was added with various signal-to-noise ratio values. The results are presented in Figures (6-9).

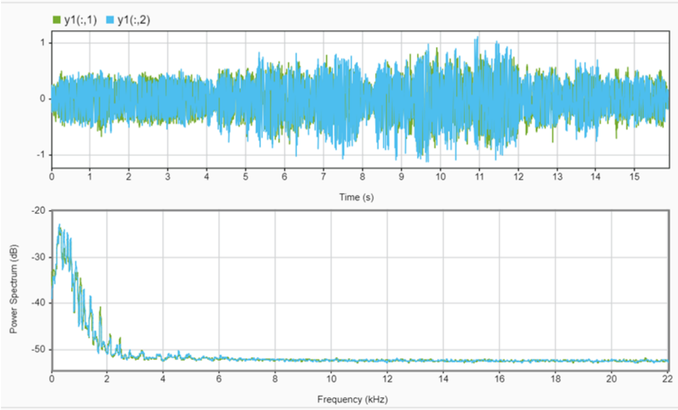


Fig. 10. Temporal and spectral diagrams of the noisy signal with the embedded message at a signal-to-noise ratio of 20 dB

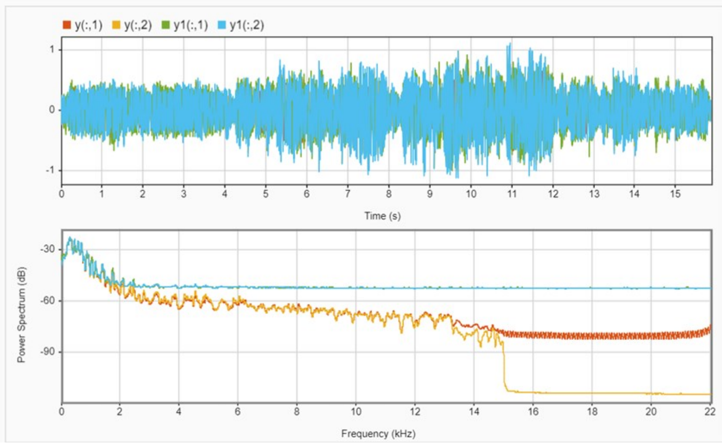
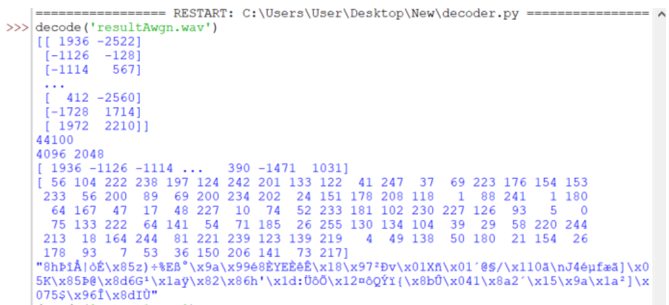


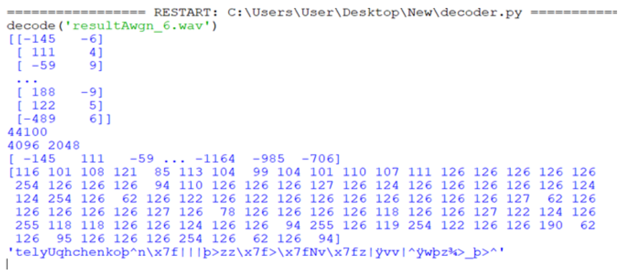
Fig 11. Comparison of the noisy signal with the embedded message and the regular signal with the embedded message

Were, *y* –audio signal file with the embedded message; *y1* – noisy signal with the embedded message at a signal-to-noise ratio of 20 dB.



```
================= RESTART: C:\Users\User\Desktop\New\decoder.py =================
>>> decode('resultAwgn.wav')
[[ 1936 -2522]
 [-1126  -128]
 [-1114   567]
 ...
 [  412 -2560]
 [-1728  1714]
 [ 1972  2210]]
44100
4096 2048
[ 1936 -1126 -1114 ...   390 -1471  1031]
[ 56 104 222 238 197 124 242 201 133 122  41 247  37  69 223 176 154 153
 233  56 200  89  69 200 234 202  24 151 178 208 118   1  88 241   1 180
  64 167  47  17  48 227  10  74  52 233 181 102 230 227 126  93   5   0
  75 133 222  64 141  54  71 185  26 255 130 134 104  39  29  58 220 244
 213  18 164 244  81 221 239 123 139 219   4  49 138  50 180  21 154  26
 178  93   7  53  36 150 206 141  73 217]
```

Fig. 12 Result of message extraction at a signal-to-noise ratio of 20 dB



```
================= RESTART: C:\Users\User\Desktop\New\decoder.py ==========
decode('resultAwgn_6.wav')
[[-145   -6]
 [ 111    4]
 [ -59    9]
 ...
 [ 188   -9]
 [ 122    5]
 [-489    6]]
44100
4096 2048
[ -145   111   -59 ... -1164  -985  -706]
[116 101 108 121  85 113 104  99 104 101 110 107 111 126 126 126 126 126
 254 126 126 126  94 110 126 126 126 127 126 124 126 126 126 126 126 124
 124 254 126  62 126 122 126 122 126 126 126 126 126 126 127  62 126
 126 126 126 126 127 126  78 126 126 126 126 118 126 126 127 122 124 126
 255 118 118 126 126 124 126 126  94 255 126 119 254 122 126 126 190  62
 126  95 126 126 126 254 126  62 126  94]
'telyUqhchenkoþ^n\x7f|||þ>zz\x7f>\x7fNv\x7fz|ÿvv|^ÿwþz¾>_þ>^'
```

Fig. 13 Result of message extraction at a signal-to-noise ratio of 60 dB

```
================== RESTART: C:\Users\User\Desktop\New\decoder.py ============
decode('resultAwgn_4.wav')
[[-152    1]
 [ 115    4]
 [ -56    8]
 ...
 [ 188    0]
 [ 127   -1]
 [-496    0]]
44100
4096 2048
[ -152   115   -56 ... -1168  -984  -712]
[116 101 108 121 117 115 104  99 104 101 110 107 111 126 126 126 126 126
 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126
 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126
 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126
 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126 126
 126 126 126 126 126 126 126 126 126 126]
'telyushchenko'
```

Fig. 14 Result of message extraction at a signal-to-noise ratio of 70 dB

The obtained results of experimental studies indicate that by increasing the signal-to-noise ratio, the distortion of the audio file decreases. Additionally, it can be concluded that reading the hidden message is impossible at signal-to-noise ratios ranging from 1 dB to 70 dB. However, it becomes possible at signal-to-noise ratios above 70 dB. Thus, if an attacker attempts to distort the hidden information by adding noise, the attack will only be successful at signal-to-noise ratios in the range of 1 to 69 dB. However, this noise will be perceptible to the human ear, resulting in distortion of the audio file.

In the case of a noise attack with a signal-to-noise ratio of 70 dB or higher, the attack will not be successful, and the message can be read (Figure 14).

V. Discussion

Analysis of the data presented in Figures 3-14 allows for the following conclusions:

Firstly, the Python programming language is more optimal for writing software aimed at hiding digital watermarks due to its cross-platform compatibility, ease of writing, and sufficient number of libraries for utilization. It is difficult to implement information hiding without significant container distortion.

Secondly, the phase coding method involves replacing the original audio element with the relative phase, which serves as the hidden message. A drawback of this method is that it cannot achieve hiding a large amount of data. The probability of distorting the secret information in this method is much lower than in other investigated methods.

Another key conclusion is that the noise attack is successful only within a certain range of signal-to-noise ratios from 1 to 69 dB. In this range, the distortion of the container is significant. In the range of 70 dB and higher, if container distortion occurs at all, it is minimal and imperceptible to an outsider. Extracting the message after conducting an attack in this range is possible.

VI. Conclusion

In this article, the method of information concealment using the steganographic phase coding method has been investigated. Various sizes of embedded information and their impact on container distortion have been examined. The resilience of the hidden information to noise attacks has also been explored.

The results vividly demonstrate that the utilization of this method for information concealment is promising. The information was successfully concealed in the first segment, with the container characteristics remaining unchanged. Particularly, this pertains to human sensory perception, where container distortion remains imperceptible to the human ear. The method exhibited its best characteristics when studied against noise attacks. The resilience threshold has been determined at a level of 70 dB and above.

However, it should be noted that the information is encoded only in the first part of the signal, making this method unsuitable for concealing large amounts of data and consequently resulting in low throughput capacity.

References

[1] Y. Zhang, Y. Liu, Z. Chen, and H. Zhang, "Audio Steganography Based on Phase Coding with Improved Embedding Efficiency," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 343-353, Feb. 2019. https://doi.org/10.3724/sp.j.1087.2009.02942

[2] R. K. Jha and D. Sharma, "Phase Coding Method for Audio Steganography," in Proceedings of the 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1467-1471, Sep. 2018.

[3] Z. Liu, W. Lu, and H. Zhang, "A New Audio Steganography Method Based on Phase Coding and Key Modulation," in IEEE Access, vol. 7, pp. 35481-35493, 2019. https://doi.org/10.1109/ACCESS.2019.2906775

[4] R. Li and X. Li, "An Audio Steganography Scheme Based on Phase Coding with High Embedding Capacity," in Proceedings of the 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 10-15, Oct. 2019.

[5] J. Núñez, V. Alarcón-Aquino, and F. J. Gallegos-Funes, "Audio Steganography Using Phase Coding and Echo Hiding," in IEEE Access, vol. 7, pp. 171145-171156, 2019. https://doi.org/10.1109/ACCESS.2019.2959396

[6] Y. Yuan, S. Zhu, and L. Feng, "High-Capacity Audio Steganography Based on Phase Coding Using Spectrogram Analysis," in IEEE Access, vol. 7, pp. 123469-123479, 2019. https://doi.org/10.1109/ACCESS.2019.2934521

[7] Y. Yang and S. Jia, "Audio Steganography Using Phase Coding with a Hybrid Modulation Technique," in Proceedings of the 2019 International Conference on Electronics, Communications and Information Technology (ICECIT), pp. 53-57, Dec. 2019.

[8] R. Li and X. Li, "An Audio Steganography Scheme Based on Phase Coding with High Embedding Capacity," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1969-1981, Sept. 2015. https://doi.org/10.1109/TIFS.2015.2446164

[9] D. Kahn, "The Codebreakers: The Story of Secret Writing." Macmillan Publishing Company, New York, USA, 1996.

[10] J. R. Kim, Y. S. Moon, "A robust wavelet-based digital watermark using level-adaptive thresholding," in Proc. of the 6th IEEE Int. Conf. on Image Processing, 1999, p. 202.

[11] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," in IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 535-064, Dec. 1997. https://doi.org/10.1109/southc.1996.535064

[12] L. Von Ahn and N.J. Hopper, "Public-Key Steganography," in Advances in Cryptology: EurocryptŁ2004 (C. Cachin and J. Camenisch, eds.), vol. 3027 of Lecture Notes in Computer Science, pp. 322-339, Springer, 2004. https://doi.org/10.1007/978-3-540-24676-3_20

[13] M. Backes, C. Cachin, "Public-Key Steganography with Active Attacks," IBM Research Zurich Research Laboratory, CH-8803, Ruschlikon, Switzerland, August 26, 2004. https://doi.org/10.1007/978-3-540-30576-7_12

[14] P. Moulin, J.A. O'Sullivan, "Information-Theoretic Analysis of Information Hiding," IEEE Transactions on Information Theory, vol. 49, no. 3, pp. 563-593, March 2003. https://doi.org/10.1109/isit.2000.866309

[15] J.K. Su, J.J. Eggers, B. Girod, "Analysis of Digital Watermarks Subjected to Optimum Linear Filtering and Additive Noise Signal Processing," Special Issue on Information Theoretic Issues in Digital Watermarking, vol. 81, no. 6, pp. 1141-1175, 2001. https://doi.org/10.1016/s0165-1684(01)00038-x

[16] F. Petitcolas, R.J. Anderson, M.G. Kuhn, „Information Hiding – A Survey," Proceedings IEEE, Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, pp. 1069-1078, 1999. https://doi.org/10.1109/5.771065

[17] F. Hartung, M. Kutter, "Multimedia Watermarking Techniques," Proceedings IEEE, Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, pp. 1079-1107, 1999. https://doi.org/10.1109/5.771066

[18] M.D. Swanson, M. Kobayahi, A.H. Tewfik, "Multimedia Data-Embedding and Watermarking Strategies," Proceedings of IEEE, vol. 86, no. 6, pp. 1064-1087, 1998. https://doi.org/10.1109/5.687830

[19] T. Basar, G.J. Olsder, Dynanic Noncooperative Game Theory. SIAM Classics in Applied Mathematics, Philadelphia, PA: SIAM, 1999. https://doi.org/10.1137/1026092

[20] O. Yudin, R. Ziubina, S. Buchyk, O. Bohuslavska, and V. Teliushchenko, "Speaker's Voice Recognition Methods in High-Level Interference Conditions," in 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Jul. 2019, doi: 10.1109/ukrcon.2019.8879937.

[21] G. Langelaar, R. Lagendijk, J. Biemond, "Robust labeling methods for copy protection of images," Proc. of SPIE. Storage and Retrieval for Image and Video Databases, 1997, vol. 3022, pp. 298-309. https://doi.org/10.1117/12.263418

[22] A. Kuznetsov, A. Onikiychuk, O. Peshkova, T. Gancarczyk, K. Warwas, and R. Ziubina, "Direct Spread Spectrum Technology for Data Hiding in Audio," Sensors, vol. 22, no. 9, p. 3115, Apr. 2022, doi: 10.3390/s22093115. https://doi.org/10.3390/s22093115